CROSS-BORDER DIGITAL EVIDENCE AND DATA SOVEREIGNTY IN CRIMINAL PROCEEDINGS

Sergio Pommier Gallo, PhD.
ORCID iD: 0009-0000-7387-3943
Affiliation: Stanford University
Website: https://sergiopommiergallophd.blogspot.com

Abstract

This study examines the structural and doctrinal tensions arising from cross-border digital evidence in contemporary criminal proceedings. As data is increasingly stored in distributed cloud infrastructures, territorial principles of jurisdiction are challenged by the transnational nature of information flows. The research analyzes how data sovereignty conflicts, platform-mediated access, and jurisdictional fragmentation affect evidentiary admissibility, chain of custody, and due process guarantees. Using a comparative and interdisciplinary framework integrating criminal procedure, cyberlaw, and transnational governance, the study identifies systemic asymmetries in access to digital evidence and proposes a harmonized admissibility model grounded in procedural safeguards, evidentiary reliability, and international cooperation. The findings support the hypothesis that structural sovereignty fragmentation—rather than isolated procedural deficiencies—constitutes the primary constraint on effective and fair use of digital evidence in criminal justice systems.

Keywords: digital evidence; data sovereignty; jurisdiction; criminal procedure; due process; cybercrime; transnational law.

---

1. **Introduction**

   The digitization of social, economic, and communicative activity has transformed the evidentiary foundation of criminal law. Digital evidence—emails, metadata, cloud-stored files, platform logs—has become central to investigation and adjudication. However, unlike physical evidence, digital data

is frequently stored across multiple jurisdictions simultaneously, often under the control of private entities operating transnational infrastructures.

This structural reality disrupts the territorial logic of criminal procedure. Investigators must navigate complex legal frameworks, including mutual legal assistance treaties (MLATs), corporate compliance regimes, and conflicting national laws. As a result, the acquisition and admissibility of digital evidence are no longer purely procedural matters but are shaped by geopolitical, technological, and institutional constraints.

Research Question: How do cross-border data structures and sovereignty conflicts affect the admissibility, reliability, and procedural fairness of digital evidence in criminal proceedings?

Hypothesis (H1): Cross-border digital evidence is structurally constrained by jurisdictional fragmentation and platform-mediated access, generating systemic asymmetries that affect both prosecutorial capacity and defense rights.

---

2. **Theoretical Framework**
   This study integrates doctrines of criminal procedure with theories of sovereignty, digital governance, and transnational law.

Data sovereignty refers to the principle that data is subject to the legal regime of the territory in which it is stored. In distributed cloud environments, however, data is often fragmented across multiple jurisdictions, rendering territorial sovereignty operationally unstable.

The concept of platform sovereignty is introduced to describe the de facto regulatory authority exercised by private technology companies over data access, retention, and disclosure. Platforms act as intermediaries between state actors and digital evidence, effectively shaping the conditions under which evidence becomes available.

Additionally, the study adopts a criminological perspective on structural asymmetry, recognizing that states possess unequal capacities to access and utilize digital evidence

due to disparities in legal infrastructure, technological capability, and international cooperation.

---

3. Methodology

The research employs a qualitative-comparative doctrinal methodology.

Data sources: international legal instruments; domestic statutes; judicial decisions; institutional reports; academic literature on cybercrime and digital evidence.

Analytical approach: doctrinal analysis combined with comparative evaluation across jurisdictions.

Geographic scope: United States, European Union, and selected Latin American jurisdictions.

Variables analyzed: jurisdictional authority; access mechanisms; evidentiary admissibility; chain of custody; procedural safeguards; platform compliance.

Evidence classification:
High = codified law and judicial precedent
Medium = institutional and policy reports
Inferential = doctrinal synthesis and comparative reasoning

---

4. Results

The analysis identifies four primary structural dynamics:

(1) Jurisdictional Overlap
Multiple states may claim authority over the same dataset, generating legal conflicts and delays in evidence acquisition.

(2) Access Asymmetry
Law enforcement agencies differ significantly in their capacity to obtain digital evidence, depending on legal tools, diplomatic channels, and technical resources.

(3) Platform Mediation
Private corporations function as gatekeepers, determining access through internal policies, compliance thresholds, and data retention practices.

(4) Chain of Custody Disruption
Cross-border transfers of digital evidence introduce risks to evidentiary integrity, including incomplete documentation, metadata loss, and jurisdictional gaps.

Comparative Matrix:

United States — expansive legal instruments — extraterritorial reach — strong enforcement capacity
European Union — rights-centered regulation — strict data protection — procedural safeguards
Latin America — limited infrastructure — dependence on external cooperation — variable enforcement

These findings demonstrate that digital evidence operates within a structurally mediated system rather than a purely legal one.

---

5. Discussion

The results support the hypothesis that structural fragmentation defines the contemporary evidentiary landscape.

Jurisdictional conflicts undermine procedural clarity, often delaying investigations and creating uncertainty regarding admissibility. Evidence obtained through contested legal mechanisms risks exclusion or constitutional challenge.

Due process concerns are particularly acute. Defendants may lack access to exculpatory data located in foreign jurisdictions or controlled by private platforms, creating asymmetrical litigation conditions.

Platform sovereignty introduces an additional layer of opacity. Corporate policies—often non-transparent—affect evidence availability, effectively privatizing aspects of criminal procedure.

The study proposes that digital evidence should be treated as a structurally conditioned resource requiring enhanced procedural safeguards.

---

6. **Limitations**

   The study relies on doctrinal and secondary sources, which may not fully capture operational practices of law enforcement agencies.

Additionally, the rapid evolution of cloud technologies and platform policies may outpace existing legal frameworks.

Future research should incorporate empirical case studies, technical audits of data access mechanisms, and quantitative analysis of cross-border evidence flows.

---

7. **Conclusions**

   Cross-border digital evidence represents a structural transformation of criminal procedure.

Jurisdictional fragmentation, platform mediation, and sovereignty conflicts create systemic constraints affecting both prosecution and defense.

The study proposes a harmonized admissibility model based on three core principles:
(1) procedural transparency
(2) evidentiary reliability
(3) reciprocal international cooperation

Without structural reform, digital evidence will continue to generate inequalities and inefficiencies within criminal justice systems.

References (APA 7th)

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention).
Kerr, O. S. (2010). Computer crime law. West Academic Publishing.

Pardo, M. S., & Patterson, D. (2013). Minds, brains, and law. Oxford University Press.
Svantesson, D. J. B. (2017). Solving the Internet jurisdiction puzzle. Oxford University Press.
United Nations Office on Drugs and Crime (UNODC). (2013). Comprehensive study on cybercrime.

References (Chicago Style)

Council of Europe. 2001. Convention on Cybercrime. Budapest.
Kerr, Orin S. 2010. Computer Crime Law. St. Paul: West Academic.
Pardo, Michael S., and Dennis Patterson. 2013. Minds, Brains, and Law. Oxford: Oxford University Press.
Svantesson, Dan Jerker B. 2017. Solving the Internet Jurisdiction Puzzle. Oxford: Oxford University Press.
United Nations Office on Drugs and Crime. 2013. Comprehensive Study on Cybercrime.

License
Creative Commons Attribution 4.0 (CC BY 4.0)

Version
Preprint (submitted manuscript, not peer-reviewed)